UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,177	11/05/2003	Jiwu Jing	9896-000013	7521

27572 7590 05/01/2007

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
TURCHEN, JAMES R	
ART UNIT	**PAPER NUMBER**
2139	
MAIL DATE	**DELIVERY MODE**
05/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/702,177	JING ET AL.	
	Examiner	Art Unit	
	James Turchen	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-18 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-8 is/are rejected.

7)☒ Claim(s) 9-18 is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 22 February 2007 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-18 are pending. Claims 1, 8, 10, and 13 are amended.

Response to Arguments

Applicant's arguments with respect to claims 1-7 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1 recites the limitation "the calculation results" in third paragraph. There is insufficient antecedent basis for this limitation in the claim.

Claim 1 states "k online secret share calculators making calculation based on first sub-secret-keys pre-stored and sending out a calculation result through a second broadcast channel" then states "m online secret share combiners, each receiving the calculation results from the secret share calculators". The share calculators send out a calculation result and the secret share combiners receive "the calculation results".

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The fourth paragraph of claim 1 recites "comparing t calculation results with the equation combination representations pre-stored". It is unclear what applicant seeks to patent in the term "equation combination representations". The can be interpreted as an equation or a result.

Claim 8 recites the limitation "ca" in section H. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Frankel et al. (US 6,035,041) in view of Brickell et al. (US 6,959,394) and Brennan et al. (US 5,675,649).

Regarding claim 1: Frankel et al. discloses a digital certificate issuing system with intrusion tolerance ability, comprising:

at least one online task distributor, sending out a certificate to be signed through a first broadcast channel (column 4 lines 25-29, input processor 123 provides all of the agents 121 with information relating to the particular cryptographic service request);

k online secret share calculators (column 4 lines 20-22, agents 121), each receiving the certificate to be signed, checking correctness of the certificate to be signed (column 4 lines 38-47), making calculation based on first sub-secret-keys pre-stored, and sending out a calculation result through a second broadcast channel (column 4 lines 48-58, agents apply its individual key share (calculation));

m online secret share combiners (column 4 lines 30-34, output processor 125; m is equal to one), each receiving the calculation results from the online secret share calculators (column 4 lines 30-34, output processor 125 receives partial results from agents 121), comparing t calculation results with the equation combination representation pre-stored upon receiving at least t calculation results to get a second sub-secret-key corresponding to the t calculation results (column 4 lines 30-34, output processor 125 takes the partial results and uses an equation to combine the results), making a calculation based on the t calculation results and the second sub-secret-key

corresponding to the t calculation results, and generating a digital certificate (column 4 lines 48-58);

wherein the k, m, t are positive integers, and the t is less than the k (figure 4, agents 131, 132, 133, 134 and 135 (corresponding to k) send out 3 calculation results (137) from the five total agents).

Frankel et al. does not disclose an offline secret key distributor and pre-storing the second sub-secret-keys. Brennan et al. discloses a secure computer system distributing key shares and then shutting down the secure computer system (column 2 lines 23-31). It would have been obvious to one of ordinary skill in the art to modify the key distributor with the system of Brennan et al. to shut down upon distributing the partial keys to the agents in order to keep the key from being reconstructed from the key distributor (column 2 lines 23-31). Brickell et al. discloses storing a pre-stored piece and checking the received password with the pre-stored piece (column 5 lines 11-17). It would have been obvious to modify the key distributor with the system of Brickell et al. to pre-store pieces of the key in the output processor and check the pieces received from the agents in order to ensure no computers are compromised (column 5 lines 30-31)

Regarding claim 2: The system of claim 1, further comprising an independent output interface device connected to m secret share combiners through a third broadcast channel (column 3 lines 62 through column 4 line 2 and column 4 lines 59-62).

Regarding claim 3: The system of Claim 1, wherein an output interface device that is

connected to said m secret share combiners through the first broadcast channel is set in (column 5 lines 3-14).

said online task distributor.

Regarding claim 4: The system of claim 1, wherein all of at least one online task distributor, k online secret share calculators, m online secret share combiners and the offline secret key distributor are general-purpose computers or servers (column 5 lines 3-14).

Regarding claim 5: The system of claim 2, wherein all of at least one online task distributor, k online secret share calculators, m online secret share combiners and the offline secret key distributor are general-purpose computers or servers (column 5 lines 3-14).

Regarding claim 6: The system of Claim 3, wherein all of at least one online task distributor, k online secret share calculators, m online secret share combiners and the offline secret key distributor are general-purpose computers or servers (column 5 lines 3-14).

Regarding claim 7: The system of claim 1, wherein the first broadcast channel and the second broadcast channel are channels connected physically or independent channels not connected at all (column 3 lines 62 through column 4 line 2 and column 4 lines 59-62).

Allowable Subject Matter

Claim 8 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

Claims 9-18 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

The following is an examiner's statement of reasons for allowance: Examiner is unable to find prior art or any obvious combination thereof that discloses comparing the received results with pre-stored equivalent combination representations of the second sub-secret-keys and finding out a matching equivalent combination representation and the corresponding second sub-secret-key and then checking correctness of said certificate to be signed; after that multiplying ascending power computation results of t secret share calculators matching to the combination to obtain R; finally , computing M^(c.sub.a) based on the found ca and multiplying M^(c.sub.a) with R to obtain a digital signature S.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Turchen whose telephone number is 571-270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JRT

TAGHI ARANI
PRIMARY EXAMINER
4/21/07